Ministry of Communications and Information
An Engaged and Connected Singapore

SPEECH BY DR JANIL PUTHUCHEARY, SENIOR MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION, AT THE ISC2 SECURE ASIA PACIFIC CONFERENCE
ON 6 DEC 2023, 9.20AM

Distinguished guests,

Ladies and gentlemen,

Good morning. Thank you very much for inviting me to join you at SECURE Asia Pacific Conference, here at Marina Bay Sands. (Cybersecurity) is an important topic. It's something that we have to spend a lot of time thinking about and increasingly so, with developments in the technology space.

Developments in the Cybersecurity Landscape

2. The cybersecurity threat landscape is an evolving one. Threat actors continue to develop their capabilities and resources to try and circumvent our defences, and pose new risks to our systems. I would like to highlight three of these trends.

3. In the past year, there has been a continued increase in the speed, scale, and sophistication of attacks against our digital infrastructure.

a. Malware tools and attack frameworks have become more complex, and they are being developed for a wider range of important systems.

b. One of these tools is *Pipedream*, reported by the industrial cybersecurity firm Dragos. This is a sophisticated, modular malware, designed in 2022. It can disrupt industrial control systems (ICS) that manage public utilities and manufacturing plants. If successful, attacks could disrupt the operations of our electricity, water, oil, and gas networks, and stop our manufacturing plants from operating.

c. This type of malware is likely part of a trend where adversarial capabilities continue to evolve, ever increasing the risk of disruption.

4. The second trend is the increasing inter-dependencies and supply chain risks, across the ecosystem – the link between different chains and different transactions. More businesses and governments have adopted digital solutions and digital infrastructure for their operations. This increases their exposure to cyber threats. That increase in surface area – we know about. It has been part of our discourse and part of our thinking for some time, but the increasing inter-dependencies will throw out new volatilities – a space which we thought was relatively innocuous in the past, but as a result of increasing inter-dependencies, will become very important in the future.

a. For example, earlier this year, reports emerged that cybercriminals were exploiting an old vulnerability in the VMware ESXi servers, and using it for large-scale ransomware attacks. All vulnerabilities become increasingly salient as time passes.

b. By February 2023, more than 3,200 servers had been affected, disrupting governments, cloud service providers, and other businesses that rely on these platforms.

c. While VMware had released a security patch in 2021, these organisations had not applied it in a timely manner, and then subsequently exposed themselves to cybersecurity threats. Similar risks can emerge, will emerge, if companies do not adopt the solutions that are already there.

5. The third trend is the rapid adoption of AI.

a. The very rapid adoption of the latest round of AI tools can significantly increase the risk for systems that are operated by AI commands, or that are integrated with AI platforms. There is also the risk that our systems will face threats developed by adversarial AI models, or AI models that are misused by threat actors.

b. On 4 December 2023, we released the National AI Strategy 2.0, which sets out our commitment to understanding and addressing these concerns

as early as possible. We have been thinking about AI for some time. This is the second iteration of our national AI strategy, and we will continue to focus on what the developers in the AI space need, for our data privacy, cybersecurity and all the rest of the things that we do, supported by our digital infrastructure.

6. And against this backdrop, cybersecurity has become increasingly important. Security is the key enabler for us to capture new opportunities in the digital economy, and to do so with the trust and confidence of our consumers, our clients, our citizens.

7. This means that there are **significant opportunities for Singapore to capitalise on this growth, and to reinforce our position as a hub for excellence in the region.**

a. We are already relatively well-positioned in ASEAN, which is a region of significant opportunity. The Boston Consulting Group has projected that ASEAN's digital economy will grow to almost $1.3 trillion by 2030, more than three times the current size.

b. And enhancing our cyber workforce can attract more businesses to Singapore, providing economic opportunities and jobs for Singaporeans. This will include jobs within the cybersecurity industry.

8. So we have to be proactive in our plans for developing a robust talent pipeline for cybersecurity. This will give us a good foundation for us to be able to build and sustain our efforts to make us cyber secure here in Singapore.

A Robust Talent Pipeline

9. Developing this talent pipeline is a key priority for colleagues at the Cyber Security Agency of Singapore. **Recently, Minister Josephine Teo announced that CSA will invest $50 million in a Cybersecurity Talent, Innovation, and Growth (Cyber TIG) Plan, over the next three years.**

a. This is a comprehensive approach to ecosystem development, and ensures that multiple initiatives – past, present, and future – are coordinated and consolidated.

b. For example, under the Cyber TIG Plan, CSA will continue to provide resources and support for innovation, administered through *CyberBoost* and the *Cybersecurity Industry Call for Innovation.* These platforms provide organisations and individuals with access to the resources they need to realise their solutions to our cyber risks.

10. **Under the Talent pillar, CSA will also make a big push for the professionalisation of the cybersecurity workforce here in Singapore**. This initiative has three main benefits:

a. First, to raise the standing of the profession, through providing a framework to recognise the quality and capability of cybersecurity professionals, enhancing the appeal of the cybersecurity sector, and encouraging more people to embark on this as a lifelong career.

b. Second, to provide better frameworks and pathways for development, so that individuals get the recognition and rewards they deserve as they progress.

c. Third, to provide opportunities for international cross-recognition of the quality of your skills. CSA's efforts will take reference from existing skills frameworks, and learn from professional organisations like ISC2. We will also reference international professionalisation efforts, including the UK Cyber Security Council's Chartership scheme, which was piloted last year.

11. And we hope that everyone in the ecosystem can stand to benefit from this.

a. <u>At the organisational level</u>, increasing professionalisation of the cybersecurity workforce can raise the quality and competency of individual employees, enhancing their overall productivity. It can also help employers

articulate technical competencies and ethical standards required for each role, so that they can find the right person for the job.

b. At the national level, this approach of increasing professionalisation, increasing quality and competency will ensure that the pipeline of cybersecurity professionals remains strong and sustainable, and that we can continue to be a trusted business hub in Singapore.

12. **CSA will be conducting a study into this, starting in the first quarter of next year**, seeking the views of all our stakeholders - professionals, employers, institutes of higher learning, training and certification bodies, and professional associations.

a. CSA will use these engagements to assess the feasibility of developing this framework, and what it might entail. This is an opportunity for everyone to contribute to the future of the cybersecurity sector.

b. I will ask for your support to respond to this study with your feedback. Please give us your feedback and your input. Shape the future of cybersecurity professionals and professionalisation here in Singapore. Give us a diverse range of views that will help us chart a practical way forward, taking into account the realities of the profession that you operate in.

Partnership with ISC2

13. **I am happy to share that we are also working with ISC2 to pilot the SG Cyber Associates programme, under this Talent pillar.**

14. This collaboration and work with ISC2 provides foundational cybersecurity training for professionals without a cybersecurity background, including engineers, auditors, and lawyers. We have to constantly remind both ourselves and the rest of the world that cybersecurity is a team effort, and that everybody, including non-cyber professionals, play a part.

15. We will start with two pilots:

a. We have heard a little bit about the setting aside of 10,000 training and exam places for Singapore participants in ISC2's One Million Certified in Cybersecurity (1MCC) programme, over a period of three years. This will allow space for individuals to build their basic cybersecurity skills, or start their cybersecurity career.

b. Second: CSA is also working with the Institution of Engineers (IES) to pilot a new programme on IoT security in the next year, for IES members.

16. These programmes are pilots – we are just getting started. But these programmes will help to equip more non-cybersecurity professionals with cybersecurity competencies, aligned to their scope of work. We hope that this will provide a higher baseline for all, as we tackle the next wave of cybersecurity threats.

17. I thank ISC2 and our other close partners for their collaboration on these development initiatives.

Conclusion

18. Taken together, all these will help grow and develop that talent pipeline for Singapore, and allow us to reinforce our position as a cybersecurity hub for the region. This will ensure that we remain secure and resilient against cyber threats here in Singapore. I hope all of you will continue to participate in, support, and help us develop these talent programmes.

19. I wish you all a pleasant conference, and I hope that the discussions you have today will help you develop your own tools and capabilities.

20. Thank you once again.